CYBER THREAT INTELLIGENCE IN EDUCATIONAL TECHNOLOGY: A SYSTEMATIC REVIEW OF TRENDS, CHALLENGES, AND RESEARCH OPPORTUNITIES

ALIYU, ZAINAB IBRAHIM[1], ISMAILA, I. [2], ISAH, A. O. [3], & ABDULKADIR, O. ABDULBAKI[4]
Department of Cyber Security Science[123], Department of Telecommunications[4]
Federal University of Technology Minna Nigeria.
E-mail: zainabialiyu210@gmail.com

Abstract
The rapid digital transformation of the educational sector has led to the widespread adoption of Educational Technology (EdTech), which, while improving learning experiences, also introduces significant cybersecurity risks. This review examines the role of Cyber Threat Intelligence (CTI) in addressing these risks by combining current research on its applications, tools, frameworks, and integration with modern security architectures such as Zero Trust Architecture (ZTA) and Security Information and Event Management (SIEM). From over 35 qualitative and 20 quantitative studies published between 2019 and 2025, the review highlights key cyber threats in EdTech environments including ransomware, phishing, and insider attacks. By evaluating over 35 qualitative and 20 quantitative studies published between 2019. The study categorizes CTI types and outlines its lifecycle while exploring its integration with artificial intelligence and machine learning. Despite its advantages CTI adoption in EdTech faces challenges like limited funding, lack of skilled personnel, and fragmented IT infrastructure. Significant gaps are identified in empirical validation, human factors analysis, and integration with existing frameworks, indicating avenues for future research. The review concludes that CTI holds great promises for enhancing cybersecurity in educational institutions but requires tailored implementation strategies and more rigorous real-world evaluations to realize its full potential.

Keywords: Cyber Threat Intelligence (CTI), Educational Technology (EdTech), Zero Trust Architecture (ZTA), Machine Learning, Cybersecurity

Introduction

Educational technology (EdTech) involves the deliberate incorporation of digital tools and teaching methods designed to improve the processes of education and learning. Current research underscores that EdTech includes a variety of digital resources such as learning management systems, adaptive software, and interactive multimedia. These, together create personalized, accessible, and engaging educational experiences across a range of settings, including K-12 schools, higher education institutions, and professional development programs. Studies indicate that successfully implementing EdTech necessitates alignment with research-backed instructional strategies to enhance student outcomes and assist teachers in their roles. In addition, the responsible use of EdTech, which addresses concerns related to equity, privacy, and digital literacy, is increasingly seen as crucial for maximizing its educational benefits (Umaemah *et al.*, 2024).

The number of cybersecurity threats aimed at educational institutions has significantly increased in recent years, with a documented rise of 35% in attacks from 2023 to 2024, largely fueled by advanced ransomware operations and the targeting of interconnected third-party digital infrastructures (Lallie *et al.,* 2023). This growing trend highlights the critical need for educational organizations to strengthen their cybersecurity measures by implementing solid IT security principles, such as Zero Trust Architectures, to minimize vulnerabilities and avert data breaches. Taken together, these insights stress that educational institutions need to focus on proactive cybersecurity strategies, data privacy, and flexible defense frameworks to protect

sensitive data and ensure operational resilience in digital educational landscape (Ridha & AlDhamen, 2023). Therefore, Cyber Threat Intelligence (CTI) emerges, instead of collecting raw data about cyberattacks, CTI focuses on transforming this data into valuable and actionable insights. These insights usually encompass information about the possible perpetrators of an attack, their motivations, their methods of operation, and the specific vulnerabilities they are likely to exploit. Armed with this knowledge, organizations can make educated choices to enhance their security, shifting from a reactive approach responding only after an incident to a proactive one that seeks to anticipate and thwart attacks (Ahmad, 2024). CTI is particularly significant in the realm of EdTech, which includes the digital resources and platforms utilized in educational institutions, such as schools and universities. As the education sector increasingly depends on these technologies, it has become a more appealing target for cybercriminals.

EdTech systems often contain sensitive data, including student records, grades, financial information, and research documents, rendering them attractive to attackers (Sushama *et al.*, 2024a). By implementing cyber threat intelligence, educational institutions and EdTech providers can attain a more precise understanding of the particular threats they encounter. Equipped with this knowledge, schools and universities can take measures to bolster their defenses, safeguard sensitive information, and respond more adeptly to incidents. Additionally, CTI aids in adhering to data privacy laws, which are becoming more rigorous within the education sector. Basically, cyber threat intelligence serves as an essential resource for EdTech, as it enables educational organizations to stay ahead of cyber threats, safeguard critical information, and maintain the safety and reliability of digital learning environments for both students and educators.

This review explores the prospects, challenges and benefits of integration of Cyber Threat Intelligence in EdTech. Reviewing all the important concepts behind CTI. And also reviewing existing and most recent research related to this very area of study.

Research Questions

This study is guided by the following key questions:

i. What are the most common and damaging cyber threats affecting EdTech platforms?
ii. How is CTI currently used to detect, prevent, or respond to these threats within educational institutions?
iii. How can CTI be customized to suit the specific needs and constraints of educational environments?
iv. What future research and practical strategies are needed to improve the deployment of CTI in safeguarding EdTech?

Methodology

The research employed a comprehensive and rigorous methodology to identify, select, and analyse relevant studies within the domain. The process incorporated detailed search strategies, structured study selection procedures, and clear inclusion and exclusion criteria ensuring transparency, reproducibility, and relevance of findings. The methodology involves combining domain-specific security log analysis with threat actor profiles to robustly identify compromised applications, employing multiple analyses per application to mitigate LLM inconsistencies, and utilizing knowledge graph techniques like GraphRAG for enhanced reasoning. The system demonstrates impressive results, achieving an F-1 score of 0.90 in identifying malicious apps and reducing analyst workload by 87%, thus offering significant operational efficiency. However, limitations include the restricted diversity of applications tested and challenges related to scaling with larger datasets, as well as inherent issues with LLM inconsistencies and hallucinations. Future research aims to expand application coverage,

enhance reasoning capabilities through advanced graph-based techniques, optimize data reduction for scalability, and address LLM variability, ultimately making TIPS more robust and applicable across broader security contexts.

Information Sources and Search Strategy

The review utilized multiple electronic databases to maximize coverage, including IEEE Xplore, Scopus, ACM Digital Library, Web of Science, Google Scholar, Semantic Scholar, ResearchGate, and ScienceDirect. The search was executed using a well-defined set of keywords and phrases related to CTI, EdTech, emerging security technologies (such as Zero Trust, SIEM, threat platforms), and AI/ML applications in cybersecurity. These search terms included variations for comprehensive retrieval, for example, *"Cyber Threat Intelligence," "EdTech Security," "Threat Actor Profiling,"* and *"CTI Ontology."*

To focus on recent and relevant literature, the search was limited to articles published between 2020 and 2025. The search process was meticulously documented, including the specific search strings used for each database, to ensure transparency and facilitate reproducibility.

Furthermore, the review incorporated backward reference searching by manually reviewing reference lists of pertinent studies and forward citation tracking using Google Scholar and ResearchGate. This approach helped identify relevant studies that may not have surfaced through database searches alone.

The search results were exported to Zotero, a reference management software, for deduplication and organization. This systematic process led to an initial pool of records for further screening.

Study Selection Process

The selection process adhered to PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, as illustrated by the PRISMA diagram (Figure 1). The stages included:

1. *Identification:* A total of 70 records were identified through database searches, with none from additional sources.
2. *Screening:* After removing duplicates, 60 records remained. Titles and abstracts were initially screened—performing this step, the best candidates were selected for full-text review.
3. *Eligibility:* Full-text articles (n=55) were assessed based on eligibility criteria. Six articles were excluded for reasons such as irrelevance to CTI in EdTech (n=3), overlapping findings (n=2), and language barriers (non-English, n=2). Notably, some articles were excluded for multiple reasons.
4. *Final Inclusion:* Forty-nine studies qualified for qualitative synthesis. Eighteen of these also met criteria for quantitative synthesis (meta-analysis).
   Table 1 provides detailed counts at each stage, including reasons for exclusions.

Data Extraction Process: A systematic data extraction process was implemented to ensure precise and uniform collection of relevant information from the studies included in the review, as recorded in the table below.

Table 1: Data extraction summary

S/N	Study Characteristics	Study Objectives and Methodology	Key Findings	Recommendations and Future Research Directions
i.	Author(s)	Research questions or objectives	Security strengths and weaknesses identified	Recommendations for improving security and performance
ii.	Year of publication	Methodological approach (security analysis, performance evaluation, blockchain integration)	Performance and scalability results	Proposed updates to standards and regulations
iii.	Publication type (e.g., journal article, conference proceeding)	Various CTI concepts studied in relation to EdTech	Challenges and potential solutions for technology integration	Suggested areas for future research
iv.	Country of origin	Emerging technologies integrated (if applicable)	Regulatory landscape and standards addressed	—

Table 2: Data extraction process

Fields	Details
Study Characteristics	Author(s), Year of publication, Study objectives, Methodology.
Key Findings	Identified security strengths and weaknesses, insights on CTI implementation, technological performance data.
Recommendations & Future Directions	Suggested improvements, standards updates, or areas for further research.

The extraction process involved two steps: initial organization of data into the template, followed by synthesis and analysis to identify trends, gaps, and insights related to CTI within EdTech.

Summary of Search and Selection Outcomes

1. The initial search generated 70 records. After duplication, 60 remained.
2. Titles and abstracts led to 55 articles being deemed potentially relevant, which were then subjected to full-text review.
3. Of these, six studies were excluded because they did not meet the inclusion criteria—three for irrelevance to CTI in EdTech, two for overlapping data, and one for non-English language.
4. Final inclusion comprised 49 studies; 18 studies further contributed to meta-analytical synthesis.

The entire methodology is transparently depicted through the PRISMA and summarized in detailed tables, ensuring clarity and replicability.
This rigorous methodological approach—encompassing extensive database searching, structured study selection, and clear inclusion/exclusion criteria—enabled a comprehensive review of current research on CTI in EdTech. The combination of systematic search strategies, meticulous screening, and detailed data extraction facilitated a credible synthesis of recent advances, challenges, and future directions in the domain.

Discussion of Results

The review synthesized findings from a diverse set of studies focusing on Cyber Threat Intelligence (CTI) in educational technology (EdTech). The included studies provided insights into threat types, application challenges, technological frameworks, and implementation strategies specific to the educational sector.

Key Results from Included Studies

1. Several studies highlighted the increasing prevalence of cyber threats such as ransomware, phishing, and insider attacks targeting educational institutions. For example, Ulven & Wangen (2021) identified critical vulnerabilities in higher education environments, emphasizing the need for empirical data and security maturity models.
2. Research by Лунгол (2023) underscored region-specific threats like ransomware and phishing in Ukrainian schools under wartime conditions, stressing the importance of contextualized cybersecurity strategies.
3. Studies on application of CTI tools include Willcox & Huang (2020), who developed network models for educational data mapping, and Bulut *et al.,* (2024), who introduced the Threat Actor Informed Prioritization of Applications (TIPS). TIPS achieved high accuracy (F-1 score of 0.90) but faced limitations regarding dataset diversity and reasoning capacity, indicating ongoing challenges in scalable, reliable threat attribution systems.
4. Sudheer (2024) conducted a systematic review of ransomware techniques, emphasizing the significant operational and financial impact and the imperative for adaptive cybersecurity measures.

These findings collectively underscore the importance of integrating advanced threat detection tools, AI/ML, and formal policies to improve resilience in educational environments.

PRISMA Diagram and Study Selection Outcomes

The PRISMA diagram (Figure 1) effectively visualizes the systematic process:

1. *Records identified:* 70 via database searches; 0 from other sources.
2. *Duplicates removed:* 10, leaving 60.
3. *Screening:* Based on titles and abstracts, 55 articles remained.
4. *Full-text review:* 55 articles assessed; 6 excluded (reasons include irrelevance, duplication, and language).
5. *Final included studies:* 49 for qualitative synthesis; 18 for quantitative meta-analysis.

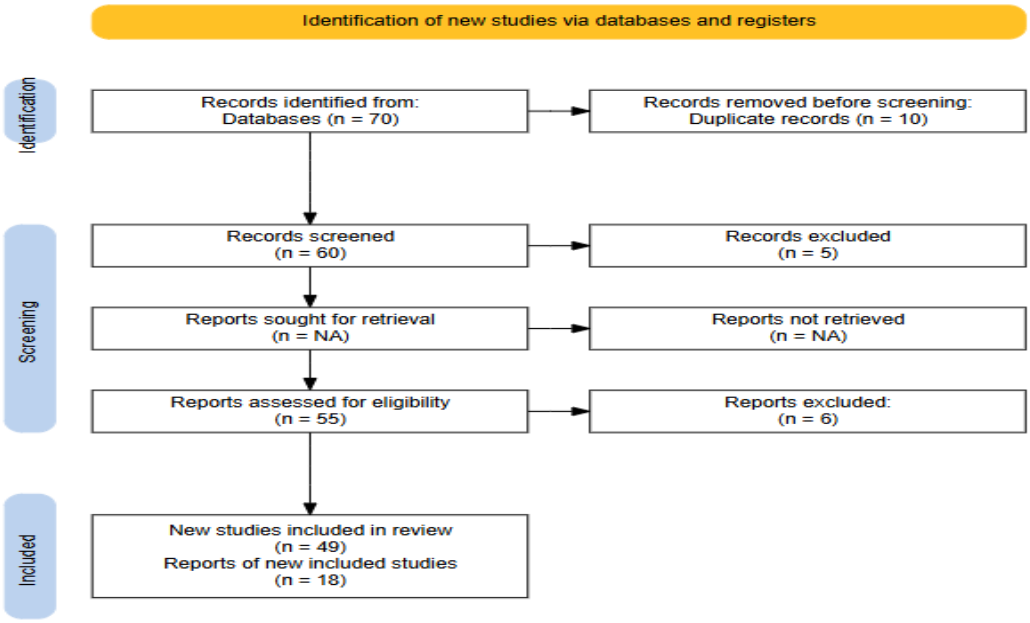

Figure 1: PRISMA diagram for systematic literature review

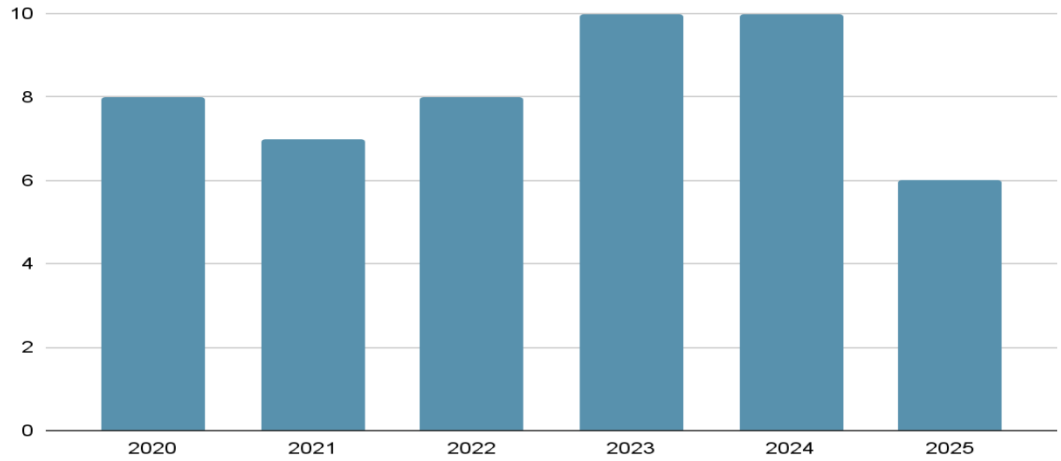

Figure 2: The Number of Publications per Year of Studies

Table 3: Data extraction summary

S/N	Study Characteristics	Study Objectives and Methodology	Key Findings	Recommendations and Future Research Directions
i.	Author(s)	Research questions or objectives	Security strengths and weaknesses identified	Recommendations for improving security and performance
ii.	Year of publication	Methodological approach (security analysis, performance evaluation, blockchain integration)	Performance and scalability results	Proposed updates to standards and regulations

Meta-Analysis Summary

The meta-analysis Table synthesized quantitative findings from 18 studies, focusing on performance metrics of CTI tools and methodologies.

Table 4: Meta-Analysis Table on summary of reviewed studies.

Study (Author & Year)	Focus Area	Methodology	Merits & Limitations
Ulven & Wangen (2021)	Cybersecurity risks in higher education	Seven-step systematic literature review of academic sources, technical reports, and white papers (post-2000)	Merits: Mapped nine HE-specific risk categories; proposed a generic threat model. Limitations: Scarcity of dataset-driven studies; publication bias; heterogeneous source depth.
Лунгол (2023)	Cyber threats in Ukrainian educational institutions under martial law	Literature review plus observations and surveys of Ukrainian institutions	Merits: In-depth, wartime-specific threat analysis; practical mitigation measures. Limitations: Ukraine-specific; relies on observational data; no longitudinal/experimental validation.
Pawar *et al.* (2024)	CTI lifecycle, sources, and implementation strategies	Framework analysis of existing CTI models, tools, open-source & proprietary feeds, and external collaborations	Merits: Clarified CTI definitions; promoted collaborative information sharing; integration guidance. Limitations: Data validation challenges; resource-intensive integration; lack of standardized sharing frameworks.
Mavroeidis & Bromander (2017)	Structured CTI ontology aligned with CTI lifecycle	Survey of taxonomies/standards; design and implementation of a modular ontology using formal logic	Merits: Enhanced semantic clarity, interoperability, and automated reasoning. Limitations: Difficulty maintaining extensibility amid evolving threats; need for broad cross-environment validation.
Papanikolaou *et al.* (2023a)	CTI Management Platform for industrial environments	Integration of public CTI (STIX 2.x) with organizational data; visualization and automation tools	Merits: Automated threat analysis; real-time situational awareness; self-healing. Limitations: Dependency on external feeds; data integration/standardization issues; scalability concerns.

Ackermann *et al.* (2023)	Integrating CTI into SIEM for industrial networks	Development of CTIExchange connector; automated ingestion and correlation of public CTI feeds into SIEM tools (Security Onion, Malcolm)	Merits: Practical enrichment of SIEM with CTI; demonstrated real-world ICS use. Limitations: Industrial focus (not educational); limited performance metrics; no extensive field deployment.
Preuveneers *et al.* (2020)	Blockchain-like distributed ledger for CTI sharing (MISP)	CP-ABE encryption; federated authentication; fine-grained access control; distributed ledger implementation with real-world threat feeds	Merits: Trustworthy, auditable, privacy-preserving sharing; ensured data provenance. Limitations: Cryptographic performance overhead; complex policy implementation; scalability challenges.
Khan (2023)	Zero Trust Architecture (ZTA) principles and implementation	Extensive literature review of academic texts, industry assessments, and case studies	Merits: Emphasized continuous verification, micro-segmentation, and reduced attack surfaces. Limitations: Complex deployment protocols; compatibility hurdles; organizational culture shifts needed.
Haque & Krishnan (2020)	Relationship-based access control for structured CTI sharing	Design of a ReBAC policy engine; cloud-hosted proof-of-concept; scenario-based access management	Merits: Innovative application of ReBAC with STIX/TAXII; flexible, policy-driven sharing. Limitations: Proof-of-concept only; lacks large-scale deployment, usability, and performance assessment.
V & Ghosh (2021)	Cybersecurity in online learning during COVID-19	Literature review of threats; vulnerability analysis of IT-enabled educational environments; best-practice recommendations	Merits: Raised awareness of remote-learning risks; practical mitigation measures (access controls, audits, training). Limitations: Conceptual only; lacks empirical validation and case studies.

Research Gaps

The document identifies several critical research gaps in the application of Cyber Threat Intelligence (CTI) within the educational technology (EdTech) sector. These gaps highlight areas where current research is insufficient and future work is needed to enhance the effectiveness and applicability of CTI in academic environments.

Contextual Specificity and Empirical Validation

I. **Industrial Focus vs. EdTech Specifics**: A significant gap is the predominant focus of current CTI research on industrial and corporate domains, with minimal adaptation to the unique structures, requirements, and limitations of educational institutions. This leads to a "contextual gap" that reduces the practical applicability of many CTI solutions in academic settings.
II. **Lack of Empirical Data**: Much of the existing literature remains theoretical, lacking empirical support from real-world implementations or case studies. This absence of solid data and long-term assessments makes it challenging to evaluate the actual efficacy of CTI solutions.
III. **Limited Generalizability**: Some studies have a specific geographic focus (e.g., Ukraine during martial law, Moodle implementation at Irbid University), which may limit the generalizability of their findings to other EdTech ecosystems, such as those in Africa or Latin America.

Integration Challenges and Human Factors

I. **Integration with Existing Security Frameworks**: A notable challenge is the difficulty in seamlessly integrating CTI with pre-existing security frameworks like Security Information and Event Management (SIEMs), Zero Trust models, and Threat Intelligence Platforms (TIPs). Discrepancies in data formats and automation processes frequently hinder smooth integration.
II. **Insufficient Human Factors Analysis**: There is a lack of research on how CTI systems influence the human factor in cybersecurity, specifically how students, faculty, and staff perceive and engage with these technologies.

Evolving Threats and Static Models

Inadequate Static Threat Models: Current research often relies on static and predetermined threat models, which do not adequately address the fluid and evolving nature of contemporary cyber threats, especially within open and rapidly changing EdTech landscapes. The rapid progression of cyber threats, particularly AI-driven attacks and ransomware, risks making current research findings quickly outdated, underscoring the need for continuous updates.

Future Research Directions

Future research in Cyber Threat Intelligence (CTI) for educational technology (EdTech) should focus on several key areas to bridge existing gaps and enhance cybersecurity in academic environments:

i. **Customization and Cost-Effectiveness:** Future studies should aim to develop CTI frameworks specifically tailored for the EdTech sector. This includes creating lightweight, affordable, and context-sensitive CTI systems suitable for schools and online learning platforms, acknowledging their unique operational and budgetary constraints
ii. **Empirical Validation and Long-Term Assessment:** There is a critical need for long-term empirical research to monitor the real-world deployment and effects of CTI tools. This involves assessing their performance, scalability, and user outcomes in actual educational settings to provide concrete evidence of their effectiveness.
iii. **Human Factors and Behavioural Aspects:** Future research should investigate the behavioral dimension of cybersecurity, specifically how CTI tools influence trust, engagement, and awareness among students, faculty, and staff within academic communities. Understanding these human factors is vital for successful adoption and sustained security practices.
iv. **Adaptive Threat Modeling and AI Integration:** nnovation in Cyber Threat

Intelligence (CTI) for the education sector should prioritize the development of real-time systems. These systems need to be capable of adaptively updating based on live data and adversarial activity. Ideally, they should be augmented by machine learning algorithms to effectively respond to the constantly changing cyber threats faced by the education sector.

Conclusion

This paper provides a detailed examination of cyber threat intelligence (CTI) and its significance in the educational sector, particularly as education shifts increasingly to online platforms. It highlights the vulnerabilities of Edtech systems to cyber-attacks and emphasizes the critical need for robust cybersecurity measures. The paper systematically reviews the integration of CTI with modern security frameworks, such as Zero Trust Architecture (ZTA) and Security Information and Event Management (SIEM), analyzing previous research to identify their advantages, limitations, and future research pathways. Ultimately, it proposes the potential for creating a secure and proactive cyber attack prevention system in education through effective CTI integration into advanced security architectures.

References

Ahmad, M. S., & V, H. (2024). The role of threat intelligence in enhancing cybersecurity posture. *International Journal of Innovative Research in Computer and Communication Engineering*, *12*(3), 1739–1746. https://doi.org/10.15680/IJIRCCE.2024.1203061

Anak Bangkong, B. L., Ehsan Rana, M., & Hameed, V. A. (2023). Overcoming the challenges of implementing cloud computing in higher education. *2023 4th International Conference on Data Analytics for Business and Industry (ICDABI)*, 341–346. https://doi.org/10.1109/ICDABI60145.2023.10629336

Anna, M. (2025). *Education-related ransomware attacks worldwide fell in 2024 | K-12 Dive*. https://www.k12dive.com/news/education-ransomware-attacks-2024-comparitech/736854/

Bhavik, P., Patel, K. B., & Niravkumar, D. (2024). revolutionizing cybersecurity with ai: predictive threat intelligence and automated response systems. *Darpan International Research Analysis,* 12(4), 1-5. https://doi.org/10.36676/dira.v12.i4.126

García-Morales, V. J., Garrido-Moreno, A., & Martín-Rojas, R. (2021). The transformation of higher education after the covid disruption: emerging challenges in an online learning scenario. *Frontiers in Psychology, 12*, 616059. https://doi.org/10.3389/fpsyg.2021.616059.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759. https://doi.org/10.3390/s21144759

Ikusika, B. (2022). A critical analysis of cybersecurity in Nigeria and the incidents of cyber-attacks on businesses/companies (SSRN Scholarly Paper No. 4165204). *Social Science Research Network.* https://papers.ssrn.com/abstract=4165204

Kante, M., Sharma, V., & Gupta, K. (2023). Mitigating ransomware attacks through cyber threat intelligence and machine learning: Survey. *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE).*

Lallie, H., Andrew, T., & Paul, S. (2023). *(PDF) Understanding cyber threats against the universities, colleges, and schools*. researchGate. https://www.researchgate.net/publication/372655992_Understanding_Cyber_Threats_Against_the_Universities_Colleges_and_Schools

Loh, P. K. K., Lee, A. Z. Y., & Balachandran, V. (2024). Towards a hybrid security framework for phishing awareness education and defense. *Future Internet.*

Martínez-Méndez, F.-J., & Lopez-Carreño, R. (2019). La paulatina adopción de ORCID para la mejora de la identidad digital de las revistas científicas españolas en acceso abierto. Investigación Bibliotecológica: Archivonomía, Bibliotecología e Información, 33(80), 73. https://doi.org/10.22201/iibi.24488321xe.2019.80.57994

Ridha, A., & AlDhamen, M. A. (2023). Cyber security awareness for education institutions. *IJARCCE*, *12*(2). https://doi.org/10.17148/IJARCCE.2023.12201

Samtani, S., & Chen, H. (2022). Linking exploits from the dark web to known vulnerabilities for proactive cyber threat intelligence: An attention-based deep structured semantic model. *MIS Quarterly,* 46(2), 911-946.

Shin, S. Y., Nejati, S., Sabetzadeh, M., Briand, L. C., Arora, C., & Zimmer, F. (2020). Dynamic adaptation of software-defined networks for IoT systems: A search-based approach. Proceedings of the IEEE/ACM 15th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, 137–148. https://doi.org/10.1145/3387939.3391603

Sushama, P., Yogita, K., Archana, G., & Manisha, P. (2024a). Cyber threat intelligence: A comprehensive overview and practical implementation. *International Journal of Advanced Research in Science, Communication and Technology*, 529–534. https://doi.org/10.48175/IJARSCT-18179.

Tanabe, R., de-Oliveira-Albuquerque, R., da-Silva-Filho, D., Alves-da-Silva, D., & Costa-Gondim, J.-J. (2023). OSINT methods in the intelligence cycle. In M. V. Garcia & C. Gordón-Gallegos (Eds.), *CSEI: International Conference on Computer Science, Electronics and Industrial Engineering (CSEI),* 678, 42–54.

Trofymenko, O., Loginova, N., Serhii, M., & Dubovoil, Y. (2022). Cyber threats in higher education. Cybersecurity: *Education, Science, Technique*, *4*(16), 76–84. https://doi.org/10.28925/2663-4023.2022.16.7684

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet,* 13(2), 39. https://doi.org/10.3390/fi13020039

Umaemah, A., Nainggolan, D. M., Halking, H., Habibatun, H., & Payage, N. (2024). The effect of EdTech integration, inclusive education policies, and continuous professional development on learning outcomes. *Journal of Social Science, 1*(4), 646–655.

https://doi.org/10.59613/g0jsct57

Varghese, V., S, M., & Kb, S. (2023). Extraction of actionable threat intelligence from dark web data. International Conference on Control, Communication and Computing (ICCC), 1-5. https://doi.org/10.1109/ICCC57789.2023.10165477

Yasin, R., Amin, S., & Yasin, M. A. (2024). Beyond the classroom: the role of technology in modern education. *Journal of Human Dynamics*, *2*(2), 69–76. https://doi.org/10.55627/jhd.002.02.0852

Yousif Yaseen, K. A. (2022). Digital education: The cybersecurity challenges in the online classroom (2019-2020). *Asian Journal of Computer Science and Technology*, *11*(2), 33–38. https://doi.org/10.51983/ajcst-2022.11.2.3450

Лунгол, О. (2023). Research of modern cyber threats in the educational environment. Актуальні Питання у Сучасній Науці, 9(15). https://doi.org/10.52058/2786-6300-2023-9(15)-630-641